DEPARTMENT OF DEFENSE
DEFENSE OFFICE OF HEARINGS AND APPEALS

In the matter of:	)	
	)	
[REDACTED]	)	ISCR Case No. 20-00230
	)	
Applicant for Security Clearance	)	

Appearances

For Government: Aubrey M. De Angelis, Esq., Department Counsel
For Applicant: *Pro se*
09/28/2021

_____

Decision

_____

MARINE, Gina L., Administrative Judge:

This case involves security concerns raised under Guideline K (Handling Protected Information), Guideline M (Use of Information Technology), Guideline E (Personal Conduct), and Guideline F (Financial Considerations). Eligibility for access to classified information is denied.

Statement of the Case

Applicant submitted a security clearance application (SCA) on August 2, 2019. On October 27, 2020, the Defense Counterintelligence and Security Agency Consolidated Adjudications Facility (DCSA CAF) sent him a Statement of Reasons (SOR) alleging security concerns under Guidelines K, M, E, and F. The DCSA CAF acted under Executive Order (EO) 10865, *Safeguarding Classified Information within Industry* (February 20, 1960), as amended; DOD Directive 5220.6, *Defense Industrial Personnel Security Clearance Review Program* (January 2, 1992), as amended (Directive); and the adjudicative guidelines (AG) implemented by the DOD on June 8, 2017.

Applicant received the SOR on November 2, 2020, answered it on a date not reflected in the record, and requested a decision on the written record in lieu of a hearing. On February 16, 2021, the Government sent Applicant a complete copy of its written case, a file of relevant material (FORM), including pleadings and evidentiary documents

identified as Items 1 through 13. He was given an opportunity to submit a documentary response setting forth objections, rebuttal, extenuation, mitigation, or explanation to the Government's evidence. He received the FORM on March 6, 2021, and did not respond or object to the Government's evidence. The case was assigned to me on June 4, 2021. Items 1 through 3 contain the pleadings in the case. Items 4 through 13 are admitted into evidence. Applicant's SOR answer included evidentiary documents that I admitted into evidence as Applicant Exhibits (AE) A through P.

Findings of Fact

Applicant, age 33, earned a high school diploma in 2005. He has taken courses at a university (University A) since 2012, but has not yet earned a degree. He served honorably in the U.S. Air Force from 2006 through 2012. He was employed as an information assurance specialist by a defense contractor (Company A) from April 2018 until July 2019; and as a cyber-information assurance analyst by another defense contractor (Company B) since July 2019. He held an active DOD security clearance while employed by Company A, but the record did not otherwise indicate his security clearance history while in the service or thereafter. Company B is sponsoring his pending security clearance application. (Item 2, 4, 6; Item 5 at 4)

The SOR alleged under Guideline K (SOR ¶¶ 1.a – 1.b), and cross alleged under Guideline M (SOR ¶¶ 2.a – 2.b) and Guideline E (SOR ¶¶ 3.a – 3.b), that, on two occasions in 2019, Applicant downloaded files from his unclassified work computer in violation of Company A policy. Also under Guideline E, the SOR alleged that Applicant falsified material facts regarding his file download activity during two different interviews in 2019, one with a Company A investigator (SOR ¶ 3.c) and one with a DOD investigator (SOR ¶ 3.d). Under Guideline F, the SOR alleged that Applicant has 11 delinquent debts totaling $48,087 (SOR ¶¶ 4.a – 4.k).

In his SOR answer, Applicant responded "I admit" to the facts alleged under Guideline K (SOR ¶¶ 1.a –1.b), which were cross alleged under Guideline M (SOR ¶¶ 2.a – 2.b) and Guideline E (SOR ¶¶ 3.a – 3.d). On the other hand, in the explanations accompanying those responses, Applicant denied the misconduct alleged in SOR ¶ 1.b. (and cross alleged in SOR ¶¶ 2.b and 3.b). Thus, I have construed his admissions to SOR ¶¶ 1.b, 2.b, and 3.b as denials. He also responded "I admit" to the facts alleged under Guideline F (SOR ¶¶ 4.a – 4.k). Regarding Guideline E, he denied the facts alleged in SOR ¶¶ 3.c and 3.d. (Items 1, 2)

SOR ¶¶ 1.a, 1.b, 2.a, 2.b, 3.a, and 3.b

On June 20, 2019, Applicant downloaded over 2,000 files from his unclassified work computer and transferred them to his personal universal serial bus (USB) drive. On June 22, 2019, he informed Company A of his resignation and intent to begin employment with Company B on July 22, 2019. On July 8, 2019, Company A discovered Applicant's high-volume file transfer and initiated an immediate investigation. (Items 6, 7)

Company A determined that the files contained on Applicant's personal USB drive included Company A proprietary information, third-party proprietary information (related

to two U.S. government programs on which Applicant was contracted to work), and export-controlled information (as designated by the International Traffic in Arms Regulations (ITAR) and the Export-Import Bank of the United States (EXIM)). Those files were marked Company A Proprietary. Company A concluded that Applicant's downloading and transfer of files to his personal USB drive was a deliberate attempt to obtain proprietary data for outside use, which was unauthorized and a direct violation of the following Company A policies: 1) Code of Conduct and 2) Protection of Company A and Third-Party Information. (Items 6, 7, 10, 11)

The investigation revealed no evidence that Applicant ever transferred those files from his USB drive to any other computer, that the USB drive ever left his personal residence where it had been stored, that any classified data resided on the USB drive, or that Applicant had any previous security incidents on his record. Nevertheless, the investigation concluded that Applicant's behavior and actions, including false statements he made during the investigation, were "Insider Threat Activity" and a risk to all Company A information systems. As a result, on July 8, 2019, Company A expedited his employment separation, seized all of Applicant's computing devices, removed his badge access, escorted him off Company A's property, and submitted an adverse statement in the DOD personnel security clearance and access database. (Items 6, 7)

On July 8, 2019, after Applicant was escorted off its property, Company A discovered information on Applicant's seized laptop which revealed that he also downloaded and transferred files from his unclassified work computer to eight computer discs on July 2, 2019. Company A determined that the files on the discs contained Company A cyber security-related tools and training, but did not provide the results of its forensic investigation of the discs which was "in progress" as of July 12, 2019, the date of its final report of the misconduct for which Applicant's separation was expedited. Neither the report nor any other record evidence indicated what, if any, conclusions that investigation formed about the presence of classified information on the discs or whether Applicant's actions in downloading or transferring the files to the discs violated any Company A policies or other rules. While acknowledging that "there is currently no evidence that Applicant copied the discs for his own use and/or removed the discs from [Company A']s premises," the Government argued in its FORM that Applicant's disc-related file transfer activity remained relevant "for the concerns it potentially raises under Guidelines K, M, and E." (Item 7)

Applicant denied that his disc-related file transfer activity was either unauthorized or violated any policies or rules. Given the timing of the discovery, Applicant was not questioned about his disc-related file transfer activity during Company A's investigation. However, he addressed it during his December 2019 security clearance interview (SI) and in his SOR answer. During his SI, Applicant explained that he never copied any files onto discs for his personal use and that his team regularly copied files onto discs in the ordinary course of business. In his SOR answer, he provided more details about the file transfer and reiterated that it was not done for his personal use. He clarified that he transferred the files (which were too voluminous to email) onto the discs to facilitate a successful transition of the systems he managed to the team member who was taking

over his position. He maintained that he gave the discs directly to his team member and never transferred the files to any other machine or device. (Item 3 at 1; Item 5 at 4)

Applicant acknowledged being aware of the proper security procedures for handling classified information when he was employed by Company A. However, he claimed that he had not had any training on handling proprietary information. He asserted that he always tried to follow security rules and that anytime he witnessed someone violating security regulations, he would counsel them and train them. As of December 2019, he had not had any security-related incidents while employed by Company B. (5 at 5; Item 7 at 4)

In September 2017, Applicant signed an employment agreement in connection with his Company A employment entitled "Employee Agreement – Proprietary Information, Inventions and Other Intellectual Property." Among the matters to which Applicant agreed were that his work product while employed by Company A was the sole and exclusive property of Company A unless expressly released in writing. He also agreed that he was prohibited from using, for his own or another's benefit, not only his own work product, but also any Company A or third-party proprietary information with which he had been entrusted or had otherwise acquired by virtue of his employment with Company A. (Item 9)

SOR ¶¶ 3.c and 3.d

In his August 2019 SCA, Applicant reported that he had been "warned, reprimanded, suspended, or disciplined" in July 2019 by Company A because he "used a USB to transfer data/files from [his] unclassified work computer." He explained: "My intentions were to bring any personal forms containing my [personally identifiable information (PII)], databases or tools I created (via excel, viso [*sic*], word, powerpoint) to build a portfolio [*sic*] I can reference prior work that assisted/streamlined tasks for my position." He asserted that the files that he transferred were "from an OPEN area" and "from [his] personal UNCLASSIFIED computer." While he acknowledged that he was told by a Company A investigator that the files he transferred were "[Company A] Proprietary," he claimed that the files he transferred "were not marked with any type of Proprietary Markings (header/footer etc)." (Item 4 at 16)

Applicant answered "Yes" on his SCA when asked whether he had "introduced, removed, or used hardware, software, or media in connection with any information technology system without authorization, when specifically prohibited by rules, procedures, or regulations" within the prior seven years. He reported July 2019 as the date of the incident. For reasons not explained in the record, Applicant did not report on his SCA that he was previously granted a security clearance. (Item 4 at 35-36, 39-40)

Applicant was interviewed twice about the facts and circumstances surrounding his Company A file transfer activity. The first interview was conducted by a Company A investigator during its July 2019 investigation (Interview 1). The second interview was conducted by a DOD investigator in December 2019 in connection with Applicant's security clearance background investigation (Interview 2). (Items 5, 7)

Company A concluded that, during Interview 1, Applicant provided false statements, including his self-described "unfamiliarity" with Company A and National Industrial Security Program Operating Manual (NISPOM) polices. When initially questioned during Interview 1, Applicant stated that he had not used any USB drive. After the question was rephrased, he stated that he was uncertain as to previous usage of a USB drive. After being reminded that Company A conducts user monitoring, Applicant reported that he discovered a USB drive on his desk. When asked to describe the data saved on the USB drive, Applicant claimed that only PII information containing social security number (SSN) data was stored on the USB drive. After he was informed that Company A's system indicated over 2,000 documents were downloaded onto the USB drive, Applicant admitted that he copied personal files and databases that he created with the intention to use them for reference purposes in the future. He later clarified that the files on the USB drive were intended to be used as references for future work outside of Company A. He acknowledged that he had taken the USB drive to his home, but maintained that he never connected it to his personal computer. (Item 7)

During Interview 1, Applicant signed a voluntary statement admitting that he "copied data from [his] unclassified [Company A] computer, with the intension [*sic*] of using files for reference purposes at a later date." He explained:

> The files were going to be a means of "referenced worked" from a coworker whom [*sic*] trained me when I initially started. The files came from my [two U.S. government programs on which Applicant worked] systems, large networks with many hours devoted to each program. The [USB drive] that was used to transfer the data has left [Company A] property/grounds, and I stored it at home. While it was there, the [USB drive] was not used. I was unaware of the [Company A] Proprietary Policy. My understanding was that it was unclassified, did not contain classified information so being able to reference prior work was not an issue. . . ." (Items 7, 8)

When initially questioned about his Company A file transfer activity during Interview 2, Applicant addressed both his USB drive and disc-related file transfer activity. He denied transferring any files onto discs for his personal use, but admitted that he transferred files to his USB drive for his personal use. He asserted that he transferred only his personal files from a folder labeled with his last name from his unclassified work computer to his USB drive around spring of 2019. He also acknowledged that he later realized that a folder labeled with the name of one of the U.S. government programs on which he worked was also copied. He did not indicate the specific timeframe that realization occurred. He claimed that he intended to use the personal files he copied to his USB drive as a portfolio to assist him with a job search, and that he had not been offered another job at the time that he transferred the files. (Item 5 at 4-5)

After initial questioning during Interview 2, Applicant was asked if there were any records or individuals that would contradict the information he provided about his USB-related file transfer activity. He replied that he believed that there were not. He was then confronted with information that the files were transferred two days prior to him submitting his resignation. Applicant denied transferring the files two days prior to submitting his

resignation and reiterated that he transferred them in the spring of 2019 before he had a job offer. But he admitted that he may have transferred his Company B offer letter from his work computer to his personal USB drive two days prior to submitting his resignation letter. (Item 5 at 5)

In his SOR answer, Applicant denied falsifying any information that he provided during Interviews 1 and 2. He stated: "To the best of my knowledge, I did not lie or attempt to withhold that I had used a USB thumb drive" from the investigator during Interview 1. He also claimed that the use of USB devices to transfer files was practiced almost daily on his Company A team and that he was "a bit confused" when the investigator explained that his file transfer activity was against Company A policy. He reaffirmed the spring of 2019 timeline he gave to the investigator during Interview 2. Additionally, he clarified that he gave the investigator "a broad timeline" of spring of 2019 because he did not recall the exact date. He affirmed that he is now certain that his initial file transfer activity occurred in "early spring of 2019." He also reaffirmed: "Again the files downloaded prior to me giving notice were personal . . . The files that were downloaded days prior to me giving my notice, was again to copy any [Company B] offer related documentation." (Item 3)

In his SOR answer, Applicant maintained that, in "early spring of 2019," he intended only to transfer a folder containing his personal files to the USB drive, including "blank tools (weekly checklist, to-do list), school/certification study material, and documents pertaining solely to [him]." He acknowledged that in "mid to late June 2019," he discovered that the personal folder he transferred to his USB drive also contained an additional folder named after one of the U.S. government programs on which he worked. He claimed that he did not intentionally transfer that additional folder as he knew that it contained information that did not pertain to him. The record did not indicate when or if he notified Company A of that discovery prior to confrontation. (Item 3)

SOR ¶¶ 4.a through 4.k

Applicant's admissions and his credit reports confirm the 11 debts alleged in the SOR totaling $48,087, including four utility accounts totaling $533; six federal student-loan accounts totaling $31,894: and a $15,660 charged-off automobile loan. (Items 3, 12, 13)

Applicant paid the automobile-loan account in September 2018 (SOR ¶ 4.k) and three of the four utility accounts alleged in SOR ¶¶ 4.a through 4.d. He paid the debt alleged in SOR ¶ 4.d ($26) in November 2020. The record does not indicate when he paid the debts alleged in SOR ¶¶ 4.b ($108) and 4.c ($332). Applicant did not establish that the debt alleged in SOR ¶ 4.a ($67) was either paid or disputed as claimed in his SOR answer. In fact, one of the documents he provided corroborated that allegation. (AE K through P; GE 5 at 8; GE 13 at 2-3)

In his August 2019 SCA, Applicant reported that he owed $7,000 to University A for unpaid tuition that was not covered by his GI Bill. He estimated that the delinquency began in July 2017. He planned to pay the balance once he determined which collection agency was holding the debt. During his December 2019 SI, he revealed that he received

a phone call in October 2019 advising him that he owed the U.S. Department of Education (USDOE) over $40,000 (and not $7,000 to University A). He denied receiving any delinquency or collection notices prior to that phone call, and believed any such notices must have been sent to either a wrong or prior address. He asserted, without providing corroborating documents, that he initiated a plan in October 2019 to pay $5 per month towards his USDOE debt and was current with those payments as of December 2019. (Item 4 at 37-38; Item 5 at 3-6)

In February 2020, Applicant entered into an agreement to rehabilitate his federal student-loan accounts with a collection agent for the USDOE, including the six accounts alleged in the SOR (SOR ¶¶ 4.e through 4.j) and one account that was not alleged. At that time, the total amount due for all seven accounts was $45,170. He agreed to make at least nine monthly payments of $352 beginning February 2020, and expected to have his accounts fully rehabilitated by November 2020. In his May 2020 response to interrogatories, he claimed that he was current with those payments and had reduced the balance to approximately $37,000. Applicant did not provide any corroborating documents to show that any payments were made or that the accounts have been fully rehabilitated. The information reported about these accounts on his January 2021 credit report did not establish that they have been rehabilitated or otherwise resolved. (AE J; Item 3; Item 5 at 8)

Applicant attributed his indebtedness to the fact that his GI Bill had "run out" as he was finishing his degree with University A and did not cover the entirety of his expenses as he anticipated. Without indicating to what year(s) he was referring, he asserted that he was "unable to pay any amount" towards his debts due to underemployment with an annual salary of $45,000, which he used to pay for his living expenses. He claimed that he has "made a point to get [himself] out of debt and work on [his] credit" since becoming employed by Company B, with an annual salary that increased by "more than double." He reported that he successfully increased his credit score from "very poor to good." The record did not otherwise specify his relevant income history and expenses, or other details about his overall financial stability. It also did not indicate whether he had any financial counseling or the extent to which the COVID-19 pandemic may have impacted his finances. (Item 3; Item 5 at 8)

Whole Person Concept

Applicant's work performance and character are highly regarded by nine individuals who wrote reference letters on his behalf. None of those individuals signified that they were aware of the facts alleged in the SOR or Applicant's USB-related file transfer activity. (AE A – I). Applicant asserted that three of the individuals who were Company A coworkers (AE A, C, F) were aware of that activity. (Item 5 at 5) However, the extent of that awareness was not indicated in the record. Two of those three Company A coworkers now work with Applicant at Company B (AE A, C).

During his Air Force service, Applicant served as an Assistant Non-Commissioned Officer in Charge (NCO) of Security Forces Training and alternate security manager (SM). His duties as SM included creating security policies and regulations. He also was

entrusted with the responsibility of protecting the security clearance information of over 7,000 airman. His supervisor stated that Applicant was "always very respectful of classified information and was a stickler of rules and regulations." (AE D)

Policies

"[N]o one has a 'right' to a security clearance." (*Department of the Navy v. Egan*, 484 U.S. 518, 528 (1988)). As Commander in Chief, the President has the authority to "control access to information bearing on national security and to determine whether an individual is sufficiently trustworthy to have access to such information." (*Egan* at 527). The President has authorized the Secretary of Defense or his designee to grant applicants eligibility for access to classified information "only upon a finding that it is clearly consistent with the national interest to do so." (EO 10865 § 2)

Eligibility for a security clearance is predicated upon the applicant meeting the criteria contained in the AG. These guidelines are not inflexible rules of law. Instead, recognizing the complexities of human behavior, an administrative judge applies these guidelines in conjunction with an evaluation of the whole person. An administrative judge's overarching adjudicative goal is a fair, impartial, and commonsense decision. An administrative judge must consider all available and reliable information about the person, past and present, favorable and unfavorable.

The Government reposes a high degree of trust and confidence in persons with access to classified information. This relationship transcends normal duty hours and endures throughout off-duty hours. Decisions include, by necessity, consideration of the possible risk that the applicant may deliberately or inadvertently fail to safeguard classified information. Such decisions entail a certain degree of legally permissible extrapolation about potential, rather than actual, risk of compromise of classified information.

Clearance decisions must be made "in terms of the national interest and shall in no sense be a determination as to the loyalty of the applicant concerned." (EO 10865 § 7). Thus, a decision to deny a security clearance is merely an indication the applicant has not met the strict guidelines the President and the Secretary of Defense have established for issuing a clearance.

Initially, the Government must establish, by substantial evidence, conditions in the personal or professional history of the applicant that may disqualify the applicant from being eligible for access to classified information. The Government has the burden of establishing controverted facts alleged in the SOR. (*Egan*, 484 U.S. at 531). "Substantial evidence" is "more than a scintilla but less than a preponderance." (*See v. Washington Metro. Area Transit Auth.*, 36 F.3d 375, 380 (4th Cir. 1994)). The guidelines presume a nexus or rational connection between proven conduct under any of the criteria listed therein and an applicant's security suitability. ISCR Case No. 15-01253 at 3 (App. Bd. Apr. 20, 2016). Once the Government establishes a disqualifying condition by substantial evidence, the burden shifts to the applicant to rebut, explain, extenuate, or mitigate the facts. (Directive ¶ E3.1.15). An applicant has the burden of proving a mitigating condition,

and the burden of disproving it never shifts to the Government. (ISCR Case No. 02-31154 at 5 (App. Bd. Sep. 22, 2005))

An applicant "has the ultimate burden of demonstrating that it is clearly consistent with the national interest to grant or continue his security clearance." (ISCR Case No. 01-20700 at 3 (App. Bd. Dec. 19, 2002)). "[S]ecurity clearance determinations should err, if they must, on the side of denials." (*Egan*, 484 U.S. at 531; AG ¶ 2(b))

Analysis

Guideline K: Handling Protected Information

That security concern under this guideline is set out in AG ¶ 33:

> Deliberate or negligent failure to comply with rules and regulations for handling protected information, which includes classified and other sensitive government information and proprietary information, raises doubts about an individual's trustworthiness, judgment, reliability, or willingness and ability to safeguard such information, and is a serious security concern.

Applicant's unauthorized transfer of proprietary and sensitive files from his unclassified work computer to his personal USB drive establishes the following disqualifying conditions under Guideline K regarding the facts alleged in SOR ¶ 1.a:

> AG ¶ 34(b): collecting or storing protected information in any unauthorized location;
>
> AG ¶ 34(c): loading, drafting, editing, modifying, storing, transmitting, or otherwise handling protected information, including images, on any unauthorized equipment or medium; and
>
> AG ¶ 34(g): any failure to comply with rules for the protection of classified or sensitive information.

The Government did not meet its burden to establish any disqualifying condition under this guideline regarding the facts alleged in SOR ¶ 1.b. The Government acknowledged in its FORM that "there is currently no evidence that Applicant copied the discs for his own use and/or removed the discs from [Company A']s premises." Moreover, the record established only that Company A initiated a forensic investigation after discovering that Applicant downloaded and transferred files to the eight discs. The results of that investigation (including whether Applicant's actions were unauthorized or otherwise violated either Company A's policies or any other rules) were not indicated in the record. Thus, I find SOR ¶ 1.b in Applicant's favor.

Having considered all of the factors set forth in AG ¶ 35 that could mitigate the concern under this guideline, I find the following relevant:

AG ¶ 35(a): so much time has elapsed since the behavior, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

AG ¶ 35(c): the security violations were due to improper or inadequate training or unclear instructions; and

AG ¶ 35(d): the violation was inadvertent, it was promptly reported, there is no evidence of compromise, and it does not suggest a pattern.

Applicant downloaded over 2,000 files from his unclassified work computer and transferred them to his personal USB drive two days before submitting his resignation. That activity was not authorized by Company A. Applicant's inconsistent statements and attempts to frame his actions as innocuous are directly at odds with persuasive record evidence.

Applicant signed an agreement outlining his responsibilities for handling proprietary information. Moreover, his background and experience together with his efforts to downplay his conduct indicate that he knew that actions were prohibited, regardless of whether he received specialized training on handling proprietary information. The sheer number of downloaded files supports a conclusion that Applicant was transferring more than merely his personal non-proprietary files and Company B offer-related documents.

Applicant's mishandling of protected information while employed at Company A raises a security concern about his willingness and ability to properly handle protected information going forward. Applicant's actions were deliberate, recent, and serious. His repeated lack of candor further undermines confidence that his misconduct is unlikely to recur and does not cast doubt on his current reliability, trustworthiness, or good judgment. AG ¶¶ 35(a), (c), and (d) are not established.

Guideline M: Use of Information Technology

The security concern under this guideline is set out in AG ¶ 39:

Failure to comply with rules, procedures, guidelines, or regulations pertaining to information technology systems may raise security concerns about an individual's reliability and trustworthiness, calling into question the willingness or ability to properly protect sensitive systems, networks, and information. Information Technology includes any computer-based, mobile, or wireless device used to create, store, access, process, manipulate, protect, or move information. This includes any component, whether integrated into a larger system or not, such as hardware, software, or firmware, used to enable or facilitate these operations.

Applicant's unauthorized transfer of proprietary and sensitive files from his unclassified work computer to his personal USB drive also establishes the following disqualifying conditions under Guideline M regarding the facts alleged in SOR ¶ 2.a:

> AG ¶ 40(d): downloading, storing, or transmitting classified, sensitive, proprietary, or other protected information on or to any unauthorized information technology system;
>
> AG ¶ 40(e): unauthorized use of any information technology system; and
>
> AG ¶ 40(f): introduction, removal, or duplication of hardware, firmware, software, or media to or from any information technology system when prohibited by rules, procedures, guidelines, or regulations or when otherwise not authorized.

Incorporating my comments under Guideline K, the Government did not meet its burden to establish any disqualifying condition under this guideline regarding the facts the facts alleged in SOR ¶ 2.b. Thus, I find SOR ¶ 2.b in Applicant's favor.

Having considered all of the factors set forth in AG ¶ 41 that could mitigate the concern under this guideline, I find the following relevant:

> AG ¶ 41(a): so much time has elapsed since the behavior happened, or it happened under such unusual circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment.

AG ¶ 41(a) was not established for the reasons articulated under Guideline K.

Guideline E: Personal Conduct

The concern under this guideline is set out in AG ¶ 15:

> Conduct involving questionable judgment, lack of candor, dishonesty, or unwillingness to comply with rules and regulations can raise questions about an individual's reliability, trustworthiness, and ability to protect classified or sensitive information. Of special interest is any failure to cooperate or provide truthful and candid answers during national security investigative or adjudicative processes. The following will normally result in an unfavorable national security eligibility determination, security clearance action, or cancellation of further processing for national security eligibility:
>
> > (a) refusal, or failure without reasonable cause, to undergo or cooperate with security processing, including but not limited to meeting with a security investigator for subject interview, completing security forms or releases, cooperation with

> medical or psychological evaluation, or polygraph examination, if authorized and required; and
>
> (b) refusal to provide full, frank, and truthful answers to lawful questions of investigators, security officials, or other official representatives in connection with a personnel security or trustworthiness determination.

Applicant's unauthorized transfer of proprietary and sensitive files from his unclassified work computer to his personal USB drive also establishes the general concerns involving questionable judgment and unwillingness to comply with rules and regulations and the following specific disqualifying condition under Guideline E regarding the facts alleged in SOR ¶ 3.a:

> AG ¶ 16(f): violation of a written or recorded commitment made by the individual to the employer as a condition of employment.

Incorporating my comments under Guideline K, the Government did not meet its burden to establish any disqualifying condition under this guideline regarding the facts alleged in SOR ¶ 3.b. Thus, I find SOR ¶ 3.b in Applicant's favor.

Applicant's deliberate lack of candor about his unauthorized file transfer activity during Interviews 1 and 2 further substantiates the general concerns under Guideline E, and also establishes the following additional specific disqualifying conditions:

> AG ¶ 16(b): deliberately providing false or misleading information; or concealing or omitting information, concerning relevant facts to an employer, investigator, security official, competent medical or mental health professional involved in making a recommendation relevant to a national security eligibility determination, or other official government representative; and
>
> AG ¶ 16(d): credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but which, when combined with all available information, supports a whole-person assessment of questionable judgment, untrustworthiness, unreliability, lack of candor, unwillingness to comply with rules and regulations, or other characteristics indicating that the individual may not properly safeguard classified or sensitive information. This includes, but is not limited to, consideration of: (1) untrustworthy or unreliable behavior to include breach of client confidentiality, release of proprietary information, unauthorized release of sensitive corporate or government protected information; (2) any disruptive, violent, or other inappropriate behavior; (3) a pattern of dishonesty or rule violations; and (4) evidence of significant misuse of Government or other employer's time or resources.

When a falsification allegation is controverted, the Government has the burden of proving it. An omission, standing alone, does not prove falsification. An administrative judge must consider the record evidence as a whole to determine an applicant's state of mind at the time of the omission. ISCR Case No. 03-09483 at 4 (App. Bd. Nov. 17, 2004). An applicant's education and experience are relevant to determining whether a failure to disclose relevant information on a security clearance application was deliberate. (ISCR Case No. 08-05637 (App. Bd. Sep. 9, 2010)

I did not find credible Applicant's explanations and excuses for his false and inconsistent statements during Interviews 1 and 2. Not only did Applicant exhibit poor judgment when he initially lied about using a USB drive during Interview 1, but he also did not own up to it until after much prodding by the investigator. He then proceeded to obscure the scope and intent of his file transfer activity throughout the remainder of Interview 1. Applicant similarly downplayed and quibbled about the facts and circumstances of his unauthorized file transfer activity during Interview 2, which not only further damaged his credibility but also suggested that he was aware of the potentially negative impact his actions could have on his security clearance. The record evidence as a whole, particularly in light of his background and experience, precludes a finding that he was uninformed about the proper handling of proprietary information. I find substantial evidence of an intent on the part of Applicant not only to provide false and misleading statements, but also to omit and conceal materially relevant information during Interviews 1 and 2. Therefore, AG ¶ 16(a) is established.

Having considered all of the factors set forth in AG ¶ 17 that could mitigate the concern under this guideline, I find the following relevant:

> AG ¶ 17(a): the individual made prompt, good-faith efforts to correct the omission, concealment, or falsification before being confronted with the facts; and
>
> AG ¶ 17(c): the offense is so minor, or so much time has passed, or the behavior is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the individual's reliability, trustworthiness, or good judgment; and
>
> AG ¶ 17(d): the individual has acknowledged the behavior and obtained counseling to change the behavior or taken other positive steps to alleviate the stressors, circumstances, or factors that contributed to
>
> untrustworthy, unreliable, or other inappropriate behavior, and such behavior is unlikely to recur.

Incorporating my comments under Guideline K and in reference to AG ¶ 16(a), I conclude that Applicant has failed to mitigate the security concerns raised by his unauthorized file transfer activity and lack of candor during Interviews 1 and 2. He further damaged his credibility when he persisted in misrepresenting facts on his SCA and in his SOR answer. His lack of candor during the security clearance process is particularly

egregious. A failure to give full, frank, and candid answers to the government in connection with a security clearance investigation interferes with the integrity of the industrial security program.

Applicant's actions call into question his ability or willingness to comply with laws, rules, and regulations, and reveal a willingness to place his own self-interest above his security obligations. Even assuming that he has not violated any security policies or other rules while employed by Company B, his refusal to acknowledge or accept responsibility for any intentional wrongdoing continues to undermine confidence in his reliability, trustworthiness, and judgment. Because he failed to demonstrate a sufficient pattern of reformed behavior, I am unable to conclude that this type of misconduct is behind him. AG ¶¶ 17(a), (c), and (d) are not established.

Guideline F: Financial Considerations

The concern under this guideline is set out in AG ¶ 18:

> Failure to live within one's means, satisfy debts, and meet financial obligations may indicate poor self-control, lack of judgment, or unwillingness to abide by rules and regulations, all of which can raise questions about an individual's reliability, trustworthiness, and ability to protect classified or sensitive information. Financial distress can also be caused or exacerbated by, and thus can be a possible indicator of, other issues of personnel security concern such as excessive gambling, mental health conditions, substance misuse, or alcohol abuse or dependence. An individual who is financially overextended is at greater risk of having to engage in illegal or otherwise questionable acts to generate funds . . . .

This concern is broader than the possibility that a person might knowingly compromise classified information to raise money. It encompasses concerns about a person's self-control, judgment, and other qualities essential to protecting classified information. A person who is financially irresponsible may also be irresponsible, unconcerned, or negligent in handling and safeguarding classified information. (ISCR Case No. 11-05365 at 3 (App. Bd. May 1, 2012))

Applicant's admissions and his credit reports establish the following two disqualifying conditions under this guideline: AG ¶ 19(a) (inability to satisfy debts); and AG ¶ 19(c) (a history of not meeting financial obligations).

Having considered all of the factors set forth in AG ¶ 20 that could mitigate the concern under this guideline, I find the following relevant:

> AG ¶ 20(a): the behavior happened so long ago, was so infrequent, or occurred under such circumstances that it is unlikely to recur and does not cast doubt on the individual's current reliability, trustworthiness, or good judgment;

> AG ¶ 20(b): the conditions that resulted in the financial problem were largely beyond the person's control (e.g., loss of employment, a business downturn, unexpected medical emergency, a death, divorce or separation, clear victimization by predatory lending practices, or identity theft), and the individual acted responsibly under the circumstances; and
>
> AG ¶ 20(d): the individual initiated and is adhering to a good-faith effort to repay overdue creditors or otherwise resolve debts.

AG ¶¶ 20(a) and 20(d) are established to mitigate concerns raised by the debts alleged in SOR ¶¶ 4.a through 4.d and 4.k, the latter of which Applicant resolved well before it became an issue with respect to his security clearance. While Applicant did not proffer sufficient evidence to corroborate his resolution of the debt alleged in SOR ¶ 4.a, I do not find it security significant in light of the record as a whole. Thus, I find those allegations in his favor. However, Applicant failed to meet his burden to establish AG ¶ 20(a), 20(b), and 20(d) to mitigate the history of indebtedness associated with his federal student-loan debt.

Applicant's student-loan debt is significant and remains unresolved. Regardless of whether it was largely attributable to issues of underemployment or GI Bill coverage, Applicant did not meet his burden to establish that he acted responsibly to address his student-loan debt in the years since July 2017, when his accounts initially became delinquent. The extent to which other factors not indicated in the record may have impacted the repayment of Applicant's federal student-loan accounts would not preclude consideration of the overall history associated with this debt.

Applicant is credited with initiating efforts to rehabilitate his delinquent loan accounts in February 2020. However, he failed to establish that his prior inaction was reasonable. He also failed to corroborate his alleged 2019 and 2020 payments, the current status of the loan accounts, and whether they were successfully rehabilitated. The record contains scant details concerning his ability to meet his financial obligations, including the specific period when he was underemployed. Applicant did not demonstrate a meaningful track record of regular and timely payments or otherwise prove that he is able to follow through with his plan for repaying his student-loan debt. Applicant failed to establish that his indebtedness is not likely to recur and no longer casts doubt on his reliability, trustworthiness, or good judgment. I have considered that Applicant is not required to be debt-free in order to qualify for a security clearance. However, in light of the record before me, I cannot conclude that Applicant has mitigated the Guideline F concerns at this time.

Whole-Person Concept

Under AG ¶ 2(c), the ultimate determination of whether the granting or continuing of national security eligibility is clearly consistent with the interests of national security must be an overall common sense judgment based upon careful consideration of the adjudicative guidelines, each of which is to be evaluated in the context of the whole person. An administrative judge should consider the nine adjudicative process factors listed at AG ¶ 2(d):

(1) the nature, extent, and seriousness of the conduct; (2) the circumstances surrounding the conduct, to include knowledgeable participation; (3) the frequency and recency of the conduct; (4) the individual's age and maturity at the time of the conduct; (5) the extent to which participation is voluntary; (6) the presence or absence of rehabilitation and other permanent behavioral changes; (7) the motivation for the conduct; (8) the potential for pressure, coercion, exploitation, or duress; and (9) the likelihood of continuation or recurrence.

I have incorporated my comments under Guidelines K, M, E, and F in my whole-person analysis, and I have considered the factors in AG ¶ 2(d). After weighing the disqualifying and mitigating conditions under Guidelines K, M, E, and F, and evaluating all the evidence in the context of the whole person, I conclude that Applicant has not mitigated the security concerns raised by his misconduct involving failure to comply with rules and regulations for handling protected information and misuse of information technology; his lack of candor about that misconduct; and his indebtedness. Accordingly, Applicant has not carried his burden of showing that it is clearly consistent with the interests of national security to grant him eligibility for access to classified information.

Formal Findings

Formal findings on the allegations set forth in the SOR, as required by Section E3.1.25 of Enclosure 3 of the Directive, are:

Paragraph 1, Guideline K:	AGAINST APPLICANT
Subparagraph 1.a:	Against Applicant
Subparagraph 1.b:	For Applicant
Paragraph 2, Guideline M:	AGAINST APPLICANT
Subparagraph 2.a:	Against Applicant
Subparagraph 2.b:	For Applicant
Paragraph 3, Guideline E:	AGAINST APPLICANT
Subparagraph 3.a:	Against Applicant
Subparagraph 3.b:	For Applicant
Subparagraphs 3.c – 3.d:	Against Applicant
Paragraph 4, Guideline F:	AGAINST APPLICANT

Subparagraphs 4.a – 4.d:	For Applicant
Subparagraphs 4.e – 4.j:	Against Applicant
Subparagraph 4.k:	For Applicant

Conclusion

I conclude that it is not clearly consistent with the interests of national security to grant Applicant eligibility for access to classified information. Clearance is denied.

Gina L. Marine
Administrative Judge